Secureworks®

DATA SHEET

Penetration Testing

Validate Security Defenses Against Real-World, Simulated Attack Methods

Identify vulnerabilities and validate security defenses utilizing independent expertise, experience and perspective to enhance your security posture, reduce your risk, facilitate compliance and improve your operational efficiency.

Think Offensively to Secure Defenses

Unauthorized access to company resources using existing and new vulnerabilities is a serious security concern. Verifying that new and existing applications, networks, and systems are not vulnerable to a security risk is key to addressing these vulnerabilities before they can be utilized by unauthorized users. While vulnerability assessments are a "light touch" evaluation to identify gaps and vulnerabilities in your network, further testing is required to show how an attacker would gain access to your environment and use those systems as a base for attacks deeper into the network.

How Secureworks® Helps

The Secureworks Adversary Group approaches every Penetration Test as unique to every organization. Our methodology is performed by the industry's top security testers, leveraging our proprietary tactics and intelligence from the Secureworks Counter Threat Unit™ (CTU™) Research Team.

Penetration Tests are designed to show how an attacker would gain unauthorized access to your environment by using similar tactics and techniques. During Internal Testing, Secureworks can leverage your entire network in an effort to compromise a subset of target systems. During External Testing, Secureworks will leverage tactics such as OSINT and credential testing in an effort to compromise the target systems. Secureworks delivers the findings in a final report, and provides a customized course of action for both leadership and technical audiences.

Customer Benefits

- Gain assurance by testing internal and external security controls, including protections around high-value systems
- Gain actionable course of action for remediation
- Satisfy compliance requirements, including PCI 3.x, FFIEC, HIPAA
- Confidence knowing the latest Threat Intelligence from The Secureworks CTU Research Team was utilized
- Determine your real-world risk of compromise

What Does the Test Help You Answer

A Penetration Test identifies and demonstrates vulnerabilities, answering the question: could an attacker break into my network? The results of the test empower your organization with a new understanding and strategy to strengthen your security posture against cyber threats that uniquely affect you.

Secureworks Penetration Testing can be performed from the perspective of threats exploiting the network edge facing the Internet **(External)**, as well as from inside the network environment **(Internal)**.

Wireless Network Testing identifies what wireless devices are accessing your network and evaluates the security of your Wi-Fi infrastructure.

Testing Your People

Because your people can also pose a risk to your network, Phishing tests can identify if your employees need training to improve your security defense. For example, you may:

- Have a mature security program and want to test people as well as the network
- Need a more advanced threat simulation that more closely matches attack vectors seen in the wild (phishing + endpoint compromise)
- Need to mix phishing engagements with network penetration testing

What to Expect in Your Report

An **Executive Summary** is targeted toward a nontechnical audience — senior management, auditors, board of directors, and other concerned parties.

Detailed Findings are targeted toward technical staff and provides detailed findings and recommendations:

Engagement methodology: Details of what was performed during the engagement

Narrative: Describes the sequence of actions taken by the testers to achieve the goals of the engagement, to assist in understanding blended threats and/or dependent phases

Detailed findings and recommendations: Describes any findings, web page links for further reading, and recommendations for remediation or risk reduction. Testers supply evidence of their findings where applicable and, if possible, sufficient information to replicate the findings using publicly available tools

Solution Features

- Tailored Rules of Engagement including review of target systems for business-critical data
- Final reports containing detailed findings and executive summary
- On-premise and remote testing options
- Option to mix External Penetration Testing, Internal Penetration Testing, and Phishing to create a blended threat scenario
- Tester-driven, manual process that includes tactics used by threat actors
- Goal-based methodology ensures that systems are tested in the greater context of their environment

Phishing Results (If applicable): A section detailing the phishing attacks used and their success rate

Other Adversarial Security Testing Services

No individual, stand-alone technique provides a comprehensive picture of an organization's security. Each adversarial test has its own objectives and acceptable levels of risk. Secureworks can work with you to determine what combination of techniques you should use to evaluate your security posture and controls to identify your vulnerabilities.

- Application Security Testing
- Red Team Testing

If your organization needs immediate assistance call our **Global Incident Response Hotline (24x7x365).**
+1-770-870-6343

For more information, call **1-877-838-7947** to speak to a Secureworks security specialist
secureworks.com

About Secureworks
Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.